STEPHANIE M. HINDS (CABN 154284)
Acting United States Attorney

TOM COLTHURST (CABN 99493)
Chief, Criminal Division

LAURA VARTAIN HORN (CABN 258485)
NICHOLAS WALSH (CABN 314290)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Laura.Vartain@usdoj.gov
Nicholas.Walsh@usdoj.gov

NICHOLAS O. HUNTER (DCBN 1022355)
STEPHEN MARZEN (NYBN 2007094)
Trial Attorneys, National Security Division

950 Pennsylvania Ave., NW
Washington, DC 20530
Tel: (202) 353-3434
Fax: (202) 233-2146
Nicholas.Hunter@usdoj.gov
Stephen.Marzen@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. FUJIAN JINHUA INTEGRATED CIRCUIT CO., LTD Defendant.	CASE NO. 18-CR-00465 MMC UNITED STATES' OPPOSITION TO DEFENDANT'S MOTION IN LIMINE NO. 4 TO EXCLUDE THE FORENSIC IMAGES OF CERTAIN ELECTRONIC DEVICES The Honorable Maxine M. Chesney Hearing: January 18, 2022 at 10:00 am Courtroom 7, 19th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES

INTRODUCTION

The Court should deny Fujian Jinhua Integrated Circuit. Co., Ltd.'s (Jinhua's) motion *in limine* number four to exclude the hard drive storing forensic images of 25 electronic devices seized in Taiwan. Even with the benefit of a forensic expert, Jinhua has not identified any material change to the evidence at issue. Therefore, Jinhua's endeavor to exclude evidence that will demonstrate exfiltration of and opening of trade secrets one through eight ("the Indicted Trade Secrets") by the individual defendants and co-conspirators in the course of their work on the joint UMC-Jinhua DRAM project is unjustified. Moreover, the fact of post-seizure access by Taiwanese law enforcement has been disclosed since the early stages of discovery. Accordingly, the sweeping and last-minute remedy that Jinhua seeks fails for these reasons:

First, there is no "spoliation" by virtue of Taiwanese law enforcement's handling of the devices prior to imaging of the devices. Spoliation requires loss of material, exculpatory evidence, and Jinhua does not point to a single piece of lost, material evidence—let alone exculpatory evidence. Further, spoliation requires bad faith, and Taiwanese law enforcement complied with existing protocols of the time and thus law enforcement's handling of the seized devices prior to imaging them could not have been in bad faith, even if there had been loss of material, exculpatory evidence (which there was

Second, Jinhua's motion sweeps too broadly. Jinhua seeks to exclude the entirety of a hard drive, which is composed of the forensic images of 25 seized devices. Although there is a single storage device, the evidence should be considered in each of its component parts, which is the forensic image of each of the 25 devices contained on it. Jinhua challenges the state of the evidence of only ten of the 25 devices.

Third, for each forensic image of a seized device that the United States seeks to use to prove the case, percipient witness testimony, together with expert testimony will tie each device to the place seized. This evidence will authenticate the evidence and be sufficient to admit it.

The Court should deny Jinhua's motion and leave probing on the effect and propriety of Taiwan law enforcement's handling of the seized devices to cross-examination and argument, as these are precisely the types of issues that go to the weight of the evidence, not its admissibility.

//

BACKGROUND

I. The Devices at Issue and the Forensic Images of These Devices

In September 2018, a grand jury returned an indictment charging Fujian Jinhua Integrated Circuit Col, Ltd. ("Jinhua") and its alleged co-conspirators with various counts related to the theft of trade secrets from Micron Technology, Inc. ("Micron"). Indictment ¶ 10 (Dkt. 1). The trade secrets Jinhua and its co-conspirators allegedly stole describe the complex processes Micron uses to manufacture multiple generations of DRAM. *Id.* ¶ 12.

The indictment alleges that defendants J.T. Ho and Kenny Wang stole Micron's trade secrets when they left their jobs at Micron's Taiwan subsidiary—Micron Memory Taiwan Co., Ltd. ("MMT")—to start working at UMC in Taiwan. UMC and Jinhua contracted jointly to develop DRAM under the codename "Project M." Ho began his employment at UMC in November 2015 and brought stolen trade secrets relating to at least three generations of Micron DRAM process technology. *Id.* ¶ 24. "Ho stored the stolen Micron trade secrets . . . on one or more digital devices belonging to UMC." *Id.* Wang left his employment at Micron and began employment at UMC in April 2016. *Id.* ¶ 26. Before leaving Micron, Wang downloaded a large amount of Micron's confidential information, including trade secrets, and brought that material to UMC. *Id.* ¶ 28. While employed at UMC, Wang stored the stolen Micron trade secrets on various digital devices and on his Google Drive account. *See id.*

On February 7, 2017, investigators from the MJIB conducted searches of Kenny Wang's office at UMC's facilities and his residence and seized eight electronic devices. During execution of the warrant, MJIB investigators downloaded documents from the UMC server to one of the seized items, which was Wang's UMC laptop, also referred to in this motion and in the expert reports as "BRG003." At trial, MJIB investigators will testify about the seizure of Kenny Wang's UMC laptop and the server download to it.

Pursuant to summonses served on various Project M employees, including Kenny Wang and J.T. Ho, MJIB investigators interviewed UMC employees on February 7 and 8. MJIB investigators also interviewed a Micron employee, Yiling Chen on February 7. During this interview, Yiling Chen explained that he had hired Kenny Wang to his position at Micron and was Wang's supervisor when

Wang quit in April 2016. MJIB asked Yiling Chen questions about Micron's protections of trade secret information and Wang's access to it while at Micron. This interview was audio and visually recorded and also transcribed, and has been produced in discovery in each format.

After Ho's interviews on February 7, 2017, MJIB accompanied Ho to UMC, where Ho turned over a hard drive that he used at UMC.

On February 9, UMC employee Shuhan Huang (Emily Shuhan) turned over three more devices used by Ho and Wang to the MJIB.

On February 13, 2017, MJIB investigators interviewed Chen Yiling again. This time, they showed him several of the devices seized from Kenny Wang and J.T. Ho and asked him to review and identify files that he believed to be Micron trade secrets. Yiling Chen did that, and his statements are contained in a written report, witnessed by Taiwan law enforcement, and signed by Chen upon verification of accuracy. This interview was audio and visually recorded and also transcribed, and has been produced in discovery in each format.

On February 14, 2017, based on evidence gathered in the interviews and the devices obtained in the investigation to date, MJIB executed another search at UMC's facility.

MJIB and Taiwan prosecutors also conducted additional interviews on February 14 and 15. In further interviews, such as those with Wang and Ho, MJIB and Taiwan prosecutors were able to show files from the seized devices, based in part on what they had learned from Chen Yiling as to the significance of certain files. To show these files, they turned on the recently seized devices and used files from the devices to show certain witnesses.

Beginning on February 18, 2017 and continuing to February 21, 2017, an MJIB forensic examiner created a forensic image of each seized device, with each image constituting a folder on a single hard drive. Accordingly, there are twenty-five[1] seized electronic devices contained on a single hard drive. Jinhua seeks to exclude the hard drive containing the 25 seized devices in its entirety. The United States refers to the hard drive containing all twenty-five images as the "forensic images of the seized devices."

Additionally, a forensic examiner conducted a keyword search of those images to identify digital

[1] MJIB seized 26 devices, but one was corrupted and so only 25 were imaged.

files that likely related to stolen Micron trade secrets. The examiner stored copies of those files on a hard drive labeled "Warehouse Seized Item No. 48 portable," which the United States generally refers to in this case as "Hard Drive 48."

All of MJIB's actions occurred in their own investigation, without involvement by the United States in the execution of the search warrants, interviews, or making of the forensic images.

The United States obtained copies of (1) Hard Drive 48 and (2) the hard drive of the forensic images of the seized devices from the Taiwan Ministry of Justice pursuant to requests made under the U.S.-Taiwan Mutual Legal Assistance Agreement ("MLAA"). Taiwan provided the evidence with certificates meant to authenticate the evidence in U.S. courts under the MLAA. Taiwan provided certificates to authenticate both Hard Drive 48 and the forensic images of the seized devices. Based on the Court's rulings on December 16, 2021, witness testimony will authenticate the evidence.

The United States has interviewed MJIB investigators about the searches and seizures, as well as the forensic imaging, and provided reports of those interviews to Jinhua. The MJIB seizing agents for the relevant devices will testify about the seizures, including events such as the download of UMC server information to Wang's device (BRG003). MJIB agent testimony, including by the lead agent working on the investigation in 2017, Agent Leo Lee, will explain that the post-seizure accesses for the purposes of furthering the ongoing investigation including interviews and additional evidence gathering was permissible at the time. In addition, the forensic agent, Chien Chih-hsuan, is expected to testify that the forensic protocols satisfied Taiwan's standards in place at the time of the search. Furthermore, Agent Chien is expected to testify that the forensics showed that no trade secret files were changed when viewed. Forensic review of the devices by the experts, as discussed below, corroborates Agent Chien.

The United States provided notice of these witnesses in its Witness List filed on December 1, 2021, *see* Dkt. 257. In short, the United States intends to authenticate the image made of each seized through percipient witness testimony.

II. Expert Disclosures about the Devices

A. The United States' Forensic Expert Report

The United States provided the forensic images of the seized devices to Berkeley Research Group ("BRG"), and asked Andy Crain of BRG to do a forensic analysis and prepare an expert report. The United States disclosed Mr. Crain's report on July 1, 2021. This report was filed by Jinhua together with its motion *in limine* at Dkt. 247-1 (Exhibit F).

Of relevance to this Opposition, the United States asked Mr. Crain to review and analyze the forensic images of the seized devices to (1) identify evidence on the image of each seized devices of which UMC employee(s) were associated with each device and (2) evidence of access, such as opening and copying, of the Indicted Trade Secret documents and other Micron confidential files by UMC employees including J.T. Ho, Kenny Wang, and Neil Lee. Dkt. 247-1 (Exhibit F) at p. 4 ¶ 4.a-e.

Mr. Crain's report describes the forensic artifacts that he analyzed to reach his conclusions. As background, and generally speaking, forensic artifacts are data that show what occurred on an electronic device when a user of the device took an action. Because UMC devices used the Windows Operating System ("Windows"), the artifacts relevant to Mr. Crain's analysis are Windows artifacts. *Id.* Accordingly, artifacts relevant to Mr. Crain's analysis include those that show when a file is copied to a specific location ("file system creation date"); system files generated automatically by Windows when a user opens a document on the computer or a USB devices connected to it ("Link files"); files generated automatically by applications running on the Windows system storing a record of files opened on the computer ("Jumplist files"); and metadata embedded in user-generated documents such as Microsoft Word documents. *Id.* ¶ 4b-e. Many of these artifacts are in fact *files* that Windows automatically creates when actions are taken on the computer by a user.

In order to inform his review, Mr. Crain received other evidence in the case, including the employee user identifiers that UMC used for J.T. Ho and Neil Lee. Mr. Crain also received the file names for the indicted Trade Secrets so that he could identify their presence during his review.

Mr. Crain's forensic review set out the evidence he found on each device to attribute each device to a specific UMC employee at Attachment C to his report. See Dkt. 247-1 (Exhibit F). Through Mr.

Crain's forensics, it is possible to show in many instances which UMC user employee identifiers were attributed with certain devices. In other instances, the forensics revealed things such as accounts opened under personal login identifiers of UMC employees to on the devices. For example, forensics corroborate the MJIB's seizure records that Kenny Wang's UMC laptop was in fact tied to Kenny Wang because forensic review revealed (1) Kenny Wang's UMC user ID profile on the forensic image; (2) jump file entries tied to the profile; (3) internet history showing use of Wang's personal email addresses; and (4) other indicia tying Wang to that device.

As it concerned the United States' request that Mr. Crain's forensic review identify the Indicted Trade Secrets and forensically assess those documents, Mr. Crain was able to identify forensic events that occurred with respect to the Indicted Trade Secret files. Put simply, Mr. Crain's report details the accesses to the Indicted Trade Secrets on the devices seized at UMC, such as copying between devices and opening. In certain instances, the forensic artifacts reveal transfer of files, such as the transfer of files between devices. For example:

> Mr. Ho exfiltrated documents from Micron principally using the BRG011 device (a Transcend USB storage device). This is evidenced by the presence of Micron documents on the device bearing metadata date stamps from the time period he worked at Micron (i.e., prior to October 2015). Then, after joining UMC, Mr. Ho connected the BRG011 device to UMC computers and saved additional copies of Micron documents to the BRG014 device (a Kingston USB storage device). Then, on multiple occasions, Mr, Ho opened numerous of these Micron documents, including various of the charged trade secret files in this matter, using BRG028 (his UMC-issued laptop) and BRG012 (a second UMC laptop that he used).

Dkt. 247-1 (Exhibit F at ¶ 5). Mr. Crain's report gives an analysis for each seized device for which he found evidence of use of copying of Indicted Trade Secret documents. The United States disclosed as Exhibits P0358-P0368, ten Federal Rule of Evidence 1006 summaries of the findings contained in Mr. Crain's report, which show pervasive, repetitive access by devices associated with J.T. Ho and others to the Indicted Trade Secret documents while working on Project M. *See e.g.*, Dkt. 258 (U.S. Exhibit List) at Exhibit P037 and filed concurrent with this motion as Exhibit A.

B. Jinhua's Expert Report

On September 10, 2021, Jinhua submitted the expert report of John F. Ashley. *See* Dkt. 247-1 at Exhibit G (Ashley Report). Critically, Mr. Ashley does not challenge Mr. Crain's findings showing pre-

seizure access to the Indicted Trade Secret files.

Instead, Mr. Ashley's report explains that he found evidence of post-seizure and pre-imaging access resulting in "data alteration or deletion" by MJIB investigators on ten of the twenty-five devices. *Id.* at p.5 (Table 2). Mr. Ashley concluded that the MJIB did not follow "well-established methods for the collection" when it accessed the devices prior to making the forensic images of the seized devices.

One of the devices that Mr. Ashley opined showed post-seizure evidence of access before it was imaged was Kenny Wang's UMC laptop (referred to in Mr. Crain's report as BRG003). Mr. Ashley opined that forensic analysis showed that on February 7, 2017, the same day that MJIB seized the device, the machine was accessed and a UMC folder was copied onto the drive. *Id.* at 8. Mr. Ashley concludes that 32,688 files were added to the device when the UMC server was downloaded and accordingly "all of that overwritten data space has been destroyed included any evidence that existed thereon at the time of seizure by the MJIB." *Id.* Mr. Ashley does not say what he means by "overwritten data space has been destroyed" or how it matters or is prejudicial. Mr. Ashley's forensic review also revealed devices inserted into the laptop in the days post-seizure and prior to the forensic imaging. According to Mr. Ashley's analysis of Kenny Wang's UMC laptop (BRG003):

> Forensic analysis confirms that after the UMC Laptop was seized from Kenny Wang and in the possession of the Prosecutor and MJIB Officers, Windows File Explorer was used to navigate to and open hundreds of files on the Laptop on February 7, 8, and 13, 2017. *When files are opened in this manner, the Windows Operating system records details in the Internet Explorer Main History, showing the file path and file title, the User profile being used and the time and data that the file was opened, as reflected in my report.*

Dkt. 247-1 at 10-11) (emphasis added). Mr. Ashley's forensic review thus confirmed what has long been disclosed in discovery, which is that MJIB accessed the devices prior to imaging them in order to conduct witness interviews. Mr. Ashley's findings as it concerned this device describe how the openings of substantive files on the device "caused" a Windows Link "file" to be created on the device. In other words, Mr. Ashley details routine system files *created* when MJIB used the computer post-seizure. *Id.* Likewise, Mr. Ashley also notes that USB devices were inserted into the computer, but does not show any evidence that the devices added or deleted any content. *Id.*

The Ashley Report continues by documenting post-seizure accesses to nine additional devices.

For example, as it concerns a USB device seized from Kenny Wang on February 7, 2017, the Ashley report documents a post-seizure access prior to forensic imaging. *Id.* at 11. Here, the Ashley Report specifies that forensic analysis reveals that "90 of the files had their Last accessed time and date metadata information updated." Mr. Ashley does not claim that any information was lost or that anything besides the metadata changed as a result of this access, nor does Mr. Ashley claim that his ability to rebut the forensic findings advanced by Mr. Crain were in any way prejudiced by any potential loss of information or changed metadata.

Similarly, the Ashley Report documents post-seizure access to BRG006 (106030-06), which was a USB drive seized from Kenny Wang, and explains that on February 13, 2017, certain files had their "Last Accessed dates" updated on that date. Mr. Ashley explains that on that date, MJIB interviewed Micron witness Yiling Chen and asked him to review files. According to Mr. Ashley:

> It is apparent from the transcript of the MJIB interrogation of Micron employee Yi-Leng chen that he was actually reviewing the files that had their Last Accessed dates updated on February 13, 2017 and may also have been the person who created and then deleted the file titled Fab11_twr_materials_for_25nm_task_force_V6.pptx. The last paragraph on Page 5 of the interrogation transcript includes a list of files which he reviewed. Amongst them are [list of 3 file'. These 3 filenames are identical to three of the files that had their metadata altered on 2/13/2017.

Ashely Report at 1.C. The only instance across any of the devices that Mr. Ashley points to any specific, potential loss of data concerns this "Fab 11" document, which is not an Indicted Trade Secret, and Mr. Crain offered no opinion about that device at all.[2]

The Ashley Report continues to detail post-seizure accesses. The Ashley Report does not conclude that MJIB deleted, changed or added any Indicted Trade Secret files during post-seizure access prior to forensic imagine, or any other material information.

C. The United States' Expert Rebuttal Report

The United States asked Mr. Crain to review Mr. Ashley's report and address any of his opinions

[2] However, if asked by defense counsel about this purported deletion, Mr. Crain is expected to testify that Mr. Ashley is not correct that the identified "Fab 11" document was deleted. Instead, Mr. Crain reviewed Mr. Ashley's work and believes that the file was accessed post-seizure and he sees its presence in the forensic image and so does not believe that it was deleted, Regardless, this file is of no relevance to the United States' case, and Jinhua does not assert that the file is material, let alone materially exculpatory in any way.

in a rebuttal report, and disclosed Mr. Crain's rebuttal report on October 15, 2021 ("rebuttal report"). It is attached to this opposition as Exhibit B.

In Mr. Crain's rebuttal report, he makes the following points relevant to this Opposition. First, Mr. Crain explains that nothing in Mr. Ashley's report changes the reliability of the data from which he determined that UMC employees repeatedly accessed the indicted Trade Secret documents:

> The post-seizure access to some of the original data sources did not affect, let alone destroy, copious and reliable forensic evidence of pertinent events on those devices that occurred *prior* to seizure. In fact, all of the forensic evidence cited in the Crain Report related to pre-seizure copying and opening of the charged trade secret documents on the various devices remains unchanged by the post-seizure access described in the Ashley Disclosure.

Ex. B ¶ 10. Mr. Crain continues to explain that all of the artifacts that he relied on to assess the pre-seizure conduct were unaffected—that is, they "are not overwritten or changed." Ex. B ¶ 13. Put simply, the fact that Mr. Crain can identify data related to the pre-seizure events means that it exists and remains reliable. Indeed, as Mr. Crain noted, Mr. Ashley's findings themselves depend on this conclusion regarding the addition of forensic artifacts. For example, Mr. Ashley described a chronology of events on one device, with events spanning multiple days of post-seizure access, and despite the later events, Mr. Ashley could still opine on earlier events because the later events did not overwrite the earlier data, but simply added to it. Ex. B at n.5.

Second, Mr. Crain highlights that Mr. Ashley does not claim there were any post-seizure accesses to five of the devices about which Mr. Crain offered an opinion, each of which contain evidence of copying and/or opening of trade secret documents. Rebuttal Report at IV. Accordingly, although Jinhua seeks to exclude all 25 devices based on post-seizure accesses to ten of them, doing so sweeps into the scope of the request the forensic images of devices with no post-seizure access.

Third, Mr. Ashley's contentions that files were added and deleted post-seizure fails to tell the Court that the "files" were of two kinds. The first type of files "created" were files downloaded onto two of the devices from UMC's servers at the time the warrants were executed. The second type of "files" are routine system files that were created when Windows logged the post-seizure events on the computer, such as those that occurred post-seizure:

> Closer analysis of the other files and folders whose date/time stamps were

> updated during post-seizure access reveals a somewhat different story than what the Ashley Disclosure leads the reader to believe. For one device, BRG003, more than 93% of the files which were created during post-seizure access were the result of Taiwanese MJIB saving a copy of a network share at UMC to the device. For the other two devices, BRG009 and BRG012, all of the files and folders that were created post-seizure consist solely of system-type files (not User Documents),and created automatically via booting and operation of the computer. **And for all three devices, all of the files and folders that the Ashely Disclosure asserts were deleted during post-seizure access consist entirely of temporary and system files, rather than User documents.**

Ex. B ¶ 24 (emphasis added); see also ¶ 25. Put differently, many of the files *added* to the devices were those that MJIB downloaded and the remainder were forensic artifacts generated automatically by the post-seizure access by MJIB.

In short, Mr. Ashley does not contest Mr. Crain's findings regarding (1) attribution of the seized devices to UMC employees; and (2) the Indicted Trade Secrets on the seized devices. Instead, he details accesses post-seizure, does not assert any material changes to the forensic images of the seized devices and both the percipient witnesses and Mr. Crain are available to address these events at trial.

ARGUMENT

I. The Forensic Images Will Be Properly Authenticated and So That is Not a Reason to Exclude Them

A. Means of Authenticating the Evidence

The forensic images of twenty-five devices are contained on one hard drive, but the United States intends to authenticate the forensic images of each device as follows: (1) MJIB testimony regarding seizure; (2) MJIB testimony regarding post-seizure events, including forensic imaging. In doing so, the United States will tell the jury precisely what the evidence is: forensic images taken soon after seizure, and with the accesses knowable by witness and expert testimony. Based on the testimony, the Court will be able to find that the United States has authenticated the forensic images of each of the seized devices that it seeks to introduce.

B. The Evidence is Substantially the Same as When Seized

The law does not support Jinhua's motion to exclude the evidence. Jinhua does not offer a single case where evidence seized by law enforcement was *excluded* due to law enforcement access to the evidence prior to forensic imaging.

Federal Rule 901(a) requires that the proponent of an item of evidence "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). "The burden on the proponent is not heavy; it needs to make a prima facie showing of authenticity. The burden is met when 'sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity.'" *United States v. Hock Chee Koo,* 990 F. Supp. 2d 1115 (D. Oregon 2011) (quoting *United States v. Tank,* 200 F.3d 627, 630 (9th Cir., 2000). Satisfying the rule is a low bar. *See United States v. Nelson*, ---F. Supp. 3d ---, 2021 WL 1391591, at *14 (N.D. Cal. April 13, 2021). Under Rule 901(a), once the bar is satisfied, the probative strength of the evidence is for the jury. *Tank,* 200 F.3d at 630.

The Ninth Circuit has opined that as a matter of chain of custody, physical evidence must be in substantially the same condition as when seized. *United States v. Harrington*, 923 F. 2d 1371, 1374 (9th Cir. 1991). "The district court may admit the evidence if there is a reasonable probability the article has not been changed in important respects." *Hock Chee Koo*, 770 F. Supp. 2d at 1121-22 (quoting *Gallego v. United States,* 276 F.2d 914, 917 (9th Cir. 1960). Jinhua contends that because the MJIB accessed the seized devices after seizure, the evidence cannot satisfy Rule 901(a) because it was not substantially the same as when seized. As a factual matter, Jinhua's own expert does not show any "substantial" changes to the evidence, and does not establish changes in any important respect, and the case law does not lend support to Jinhua's overly broad exclusion request.

Jinhua relies heavily on a case from the District of Oregon for the proposition that the Court should exclude the forensic images of the seized devices. In *United States v. Hock Chee Koo*, a district court in Oregon considered challenges to electronic evidence under Rule 901(a) and admitted the evidence, with one limitation as discussed below. 923 F.2d. at 1119

In *United States v. Hock Chee Koo,* defendant moved to exclude images the FBI made of a laptop and external hard drive in a trade secret, hacking and fraud case arising out of departing employees charged with stealing trade secrets from their employer, the Hoffman Group. 923 F.2d. at 1119. The Court held a hearing on the issue of exclusion, heard fact and expert testimony, and ruled after the hearing. *Id.*

One of the departing employees, Shengbao Wu, turned his laptop into his employer, Lawrence

Hoffman, believing that Hoffman would upgrade his computer. *Id.* Instead, Hoffman had hired a computer analyst to examine it. During that examination, the analyst, Mark Hansen, created a new folder on the laptop named "private" and copied parts of that folder to a USB external hard drive using Acronis software. *Id.* The Court called that copy of the folder onto the USB drive "Acronic backup." *Id.* Meanwhile, Hoffman took Wu's computer home and turned it on and looked at it. Hoffman testified at the evidentiary hearing that he did not delete files. *Id.* at 1119-20. He also contended that the private folder contained trade secret information owned by the Hoffman Group. *Id.* at 1120. Hoffman took these actions while he was suing Wu and others.

Hoffman's actions occurred after he reported possible theft of trade secrets to the FBI, but without FBI's knowledge that Hoffman had seized Wu's laptop. *Id.* Hoffman gave the computer and the Acronis Backup to the FBI, which then made images of the laptop (the "Laptop Image") and an image of the Acronis Backup (the "Acronis Backup Image."). *Id.* The FBI kept the images and returned the laptop and Acronis Backup to Hoffman. *Id.*

Wu moved to exclude the image of each at trial on the theory, in part, that the images could not be authenticated under Rule 901 because neither image was an accurate copy of Wu's computer prior to seizure. *Id.* at 1121. The Court ruled on each separately, admitting the Acronis Backup Image for all purposes, and limiting the laptop image in one respect. *Id.* at 1121-1127.

First, the Court admitted the Acronis Backup Image over defendant's arguments that Hansen and Hoffman could have downloaded incriminating evidence and otherwise manipulated the data. *Id.* at 1124. In admitting it, the Court said that the United States could offer the image both as proof of what the FBI took into custody and as proof of the contents of parts of Wu's computer. The Court instructed that the United States had to present the evidence regarding the proof of the contents of Wu's computer "in an appropriate fashion." *Id.* at 1122. The Court considered defendant's arguments about evidence of tampering and reasoned that although the prior employer, Hoffman, may have had a motive to change the contents of the hard drive, there was no evidence that Hansen had any such motive and Hansen made the Acronis Backup Image prior to Hoffman having possession of the computer. *Id.* at 1122. The *Hock Chee Koo* Court relied on cases holding that the theoretical possibility that data had been altered does not

establish untrustworthiness. *Id.* "The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility. *Id.* at 1122-23 *quoting United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988). The Court found that the government had met the low burden of authentication as it concerned the Acronis Backup as

> a copy of what the FBI received when it took custody of the Acronis Backup. Furthermore, the Acronis Backup Image is a copy of a portion of the contents of Wu's laptop computer on the day it was seized from him. If the evidence the government introduces it with appropriate testimony of circumstantial evidence, the Acronis Backup Image will be received.

Id. at 1123 (footnote omitted).

The court in *Hock Chee Koo* admitted the Laptop Image, as well, but limited the purpose for which the United States could do so. 770 F. Supp. 2d at 1124-25. The Court found that the Laptop Image was authenticated under Rule 901(a) as a matter of what the FBI received from Hoffman, but said the United States would still need to show why that was relevant. *Id.* The Court turned to whether the Laptop Image could be admitted as evidence of what was on Wu's laptop prior to seizure by Hoffman, and here the court declined to find it authentic because it was not in substantially the same condition as when the crime was committed. *Id.* at 1125. Because of Hoffman's history with Wu, including the civil lawsuit filed a day before Hoffman took Wu's laptop under false pretenses, the court found Hoffman had a motive to change information. *Id.* Evidence presented at a hearing with testimony from a forensic examiner further supported that Hoffman tampered with the Laptop Image. For example, forensic testimony showed that *after* the Acronis Backup had been created, there had been "specific targeted wiping or intentional defragmentation of the hard drive." *Id.* (quoting defense declaration). The court noted that there was specific evidence that defendant asserted would have been on the hard drive that was not, and that he found specific evidence of deletion of one of those files: Hoffman 200601. *Id.* In short, the defense expert concluded that certain files had existed but had been deleted and overwritten. *Id.*

Here, the United States intends to tell the jury precisely what the evidence is through witnesses who will testify about the devices seized in Taiwan, how those devices were handled post-seizure and prior to imaging, and the creation of a forensic image of each device. Furthermore, the United States'

expert is prepared to testify in detail about the forensics, and can be cross-examined by Jinhua. Similarly, Mr. Ashley can testify and explain his work. In short, by virtue of being computer evidence with data available to forensic examiners, the jury can hear about the both the fact of MJIB access and what its effects were on the seized devices.

The handling of the electronic devices post-seizure in this case by the MJIB is entirely different from the handling of the devices in *Hock Chee Koo*. Here, MJIB accessed devices in the course of an ongoing investigation, as opposed to the access the *Hock Chee Koo* court confronted, which was a disgruntled employer and his hired analyst who had already sued Wu. Notwithstanding this significant and dispositive distinction, Jinhua suggests that because MJIB showed certain devices to a Micron employee, there was a possibility of tampering. This is a mere assertion with no evidentiary support. *See Bonallo*, 858 F.2d 1427 at 1436 (the possibility of alteration of data in a computer does not establish untrustworthiness). Jinhua's forensic expert does not point to any Trade Secret documents that were tampered with, altered, or placed on any of the devices post-seizure—and these events are knowable from the forensic data such that Mr. Crain can say he did not see any evidence of alteration of Trade Secret documents. Mr. Crain, like the MJIB witnesses, will be available for cross-examination. *See United States v. Catabran,* 836 F.2d 453, 458 (9th Cir. 1987) (upholding admission of computer evidence with possible inaccuracies as relevant to the weight of the evidence and any inaccuracies could be brought out on cross-exam). The Court should allow the jury to hear the evidence and weigh it.

II. Taiwan Law Enforcement Did Not Spoliate The Seized Devices

Jinhua's request to exclude the forensic images of the seized device on the grounds that they were spoliated "by the United States and its Taiwanese counterparts in the MJIB" (Dkt. 247 at 13:10) fails because there was no spoliation. Spoliation concerns destruction of material, exculpatory evidence, and there was no destruction of evidence let alone material, exculpatory evidence. There also was no bad faith by Taiwan law enforcement in the handling of the seized devices and plainly not by the United States in acquiring the evidence. In advancing the spoliation argument, Jinhua misrepresents the facts and the legal standard.

The standards for exclusion of evidence in a criminal case based on spoliation are well-settled. As

explained in *United States v. Sivilla,* the Ninth Circuit requires a defendant to make two showings before any alleged destruction of evidence rises to a Due Process violation warranting exclusion. 714 F. 3d 1168, 1172 (9th Cir. 2013). First, the defendant must show that government acted in bad faith, which "turns on the government's knowledge of the apparent exculpatory value of the evidence at the time it was lost or destroyed." *Id.* (quoting *United States v. Cooper,* 983 F.2d 928, 931 (9th Cir. 1993) (citing *Arizona v. Youngblood,* 488 U.S. 51, 56-57 (1988)). Second, the lost evidence must be "of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *Sivilla,* 714 F.3d at 1172 (quoting *California v. Tombetta*, 467 U.S. 479, 489 (1984)).

Destruction of evidence that is only potentially useful and not materially exculpatory must also have been done in bad faith in order to rise to a Due Process violation. *See Youngblood,* 488 U.S. at 57; *Sivilla,* 714 F. 3d at 1172; *United States v. Del Toro-Barboza*, 673 F.3d 1136, 1149 (9th Cir. 2012). In order to meet the definition of materiality, the evidence must have possessed an exculpatory value that was apparent before it was destroyed. *United States v. Martinez-Martinez,* 469 F. 3d 1076, 1087 (9th Cir. 2004) (finding no suggestion that law enforcement destroyed any evidence where they did not drug test defendant on an immigration offense).

Jinhua does not and cannot establish destruction of evidence or bad faith. As a threshold matter, although Jinhua repeatedly asserts that the "government and the Taiwanese authorities" knew they had to preserve evidence, to the extent Jinhua means the United States government, there was no action at all by the United States in the seizure and post-seizure access of devices at issue in this motion. The issue is whether Taiwanese law enforcement – the MJIB – destroyed evidence meeting the relevant standards and did so in bad faith. There was no destruction of evidence. In his expert report, Mr. Ashley points to only two examples of any loss: "overwritten data space" on BRG003 (Kenny Wang UMC laptop) when MJIB downloaded UMC server files to the device; and one irrelevant file on another device seized from Kenny Wang, a mobile disk (BRG006).[3] It is not clear that anything was lost, and Jinhua does not attempt to say why either one of those would be a material, exculpatory loss.

There was also no bad faith. Jinhua asserts that the "Taiwanese knew they had to preserve the

[3] Mr. Crain's review indicates that this irrelevant file was not deleted.

status quo of all the seized devices." Dkt. 247 at 13:4-6. Status quo is a term with no legal meaning in this context. Jinhua does not point to any fact that shows any loss of evidence, let alone material evidence. All Jinhua says is that the evidence is significant. *Id.* at 19:21-23. This overly broad statement sidesteps Jinhua's burden, which is to show that there was a loss of material, exculpatory evidence with no comparable substitute. The devices are significant, but there was no destruction of the devices or the information on them. Instead, the facts show that MJIB *added* files when it (1) downloaded UMC server information to one device and (2) opened documents on certain devices, which merely created system files rather that substantive files. Put directly, Jinhua's expert Mr. Ashley gave not a single fact that showed destruction of any material evidence.

Likewise, Jinhua offers no facts to support bad faith, instead again relying on generalities and no facts. Although Jinhua claims that MJIB acted in bad faith by breaching best practices, Jinhua gives no factual support to the mental state with which any MJIB investigator acted. Jinhua asserts that animus is "evident" because the forensic officer used key words provided by Micron Memory Taiwan to search the devices. The trade secrets at issue were Micron's, so plainly terms offered by Micron to describe the trade secrets would be necessary so that the MJIB would know what they were looking for. Investigators rely on victims, including victim companies in trade secret prosecutions, to provide information on the trade secrets. Further, Jinhua seeks to establish "animus" by MJIB investigators allowing a MMT employee to review the seized devices, which occurred in the presence of law enforcement. This is hardly the stuff of "animus," or—as the standard requires—bad faith. As the evidence will show, the investigation unfolded quickly, and MJIB acted quickly to ascertain the evidence it had seized, whether additional evidence could be collected, and to avoid possible destruction of evidence by the conspiracy. These were reasonable actions, and even if imaging prior to them may have been a good idea by standards in the United States, bad faith "requires more than mere negligence or recklessness." *United States v. Flyer*, 633 F.3d 911, 916 (9th Cir. 2011). Regardless, there is no evidence that it was feasible to image the devices in the course of the rapidly moving investigation. Requiring a showing of bad faith is consistent with the Supreme Court precedent that avoids placing on law enforcement "an undifferentiated and absolute duty" to collect "all material that might be of conceivable evidentiary significance in a

particular prosecution." *Youngblood*, 488 U.S. at 58; *see also United States v. Loud Hawk*, 628 F.2d 1139, 1146 (9th Cir. 1979) (recognizing suppression of evidence as a remedy to lost evidence if the defendant can show bad faith by the government and prejudice to defendant). Here, Jinhua ignores the standards and offers no factual support even in support of the lighter burdens it created and advances.

Ignoring this clear authority on the standards for spoliation in a criminal case, Jinhua points to civil cases saying that negligence—rather than bad faith—is sufficient to warrant exclusion of the evidence. Dkt. 247 at 15:13-16:20. Jinhua is a defendant in a criminal case, and cannot avail itself of civil standards in the face of clear authority from the Supreme Court and Ninth Circuit. *Cf. Loud Hawk*, 628 F.2d at 1151 (even where the government is responsible for the loss of evidence, automatic suppression would fail to "give proper recognition to the responsibility of the Government to prosecute criminal cases.") (Kennedy, J., concurring). There is no criminal case standing for the proposition that negligence is enough, but even if so, testimony by the MJIB will establish that MJIB investigators did not act negligently because they followed existing protocols in place in 2017. The agents could not act negligently, let alone in bad faith, when following existing protocols. *See id.* (no bad faith when police acted reasonably in destroying evidence).

Moreover, while it may now be a best practice in the United States to image devices prior to accessing them, that is often not a practical reality in an unfolding criminal investigation and accordingly investigation using devices occurs prior to imaging. Take, for example, the occurrence of agents on site executing a judicially authorized search warrant in this district who, prior to seizing devices, turn on the devices to ensure that the devices are within the scope of the warrant. The booting up of the laptop and checking for indicia to tie the device to the probable cause statement prior to seizing it is in fact often necessary. Or, Customs and Border Patrol officers who interview a subject and lawfully exercise their border search authority to check devices for evidence of a crime prior to seizing the devices. *Cf. United States v. Stanford*, 716 F. App'x 689 (9th Cir. 2018) (unpublished) (authentication of cell phone after CBP official manually accessed the phone). Furthermore, a presumption of regularity attaches to officers' conduct. *See Harrington*, 923 F. 2d at 1374. In light of the expected testimony that MJIB agents acted pursuant to existing protocols, this principle is particularly true. These are not sanctionable

actions that warrant exclusion, and, so while it may be a best practice to image devices prior to searching them, there is no case on facts like this one warranting the serious remedy that Jinhua seeks.

Ultimately, the real problem with Jinhua's spoliation argument is that Jinhua points to no evidence that was lost, let alone materially exculpatory evidence. And while it is not part of a spoliation argument, Jinhua also gives no facts that show tampering at all, despite its efforts to suggest that MJIB law enforcement was merely advancing Micron's interests. Jinhua should cross-examine the MJIB witnesses at trial on their practices and make any arguments it wishes to regarding those practices to the jury.

CONCLUSION

For the foregoing reasons, the United States respectfully requests that the Court deny the motion to exclude the hard drive storing the forensic images of twenty-five seized devices.

Dated: December 22, 2021

Respectfully Submitted,

STEPHANIE M. HINDS
Acting United States Attorney

/s/
LAURA VARTAIN HORN
NICHOLAS WALSH
Assistant United States Attorneys

NICHOLAS O. HUNTER
STEPHEN MARZEN
Trial Attorneys, National Security Division

EXHIBIT A

Indicted Trade Secret 1 (7)

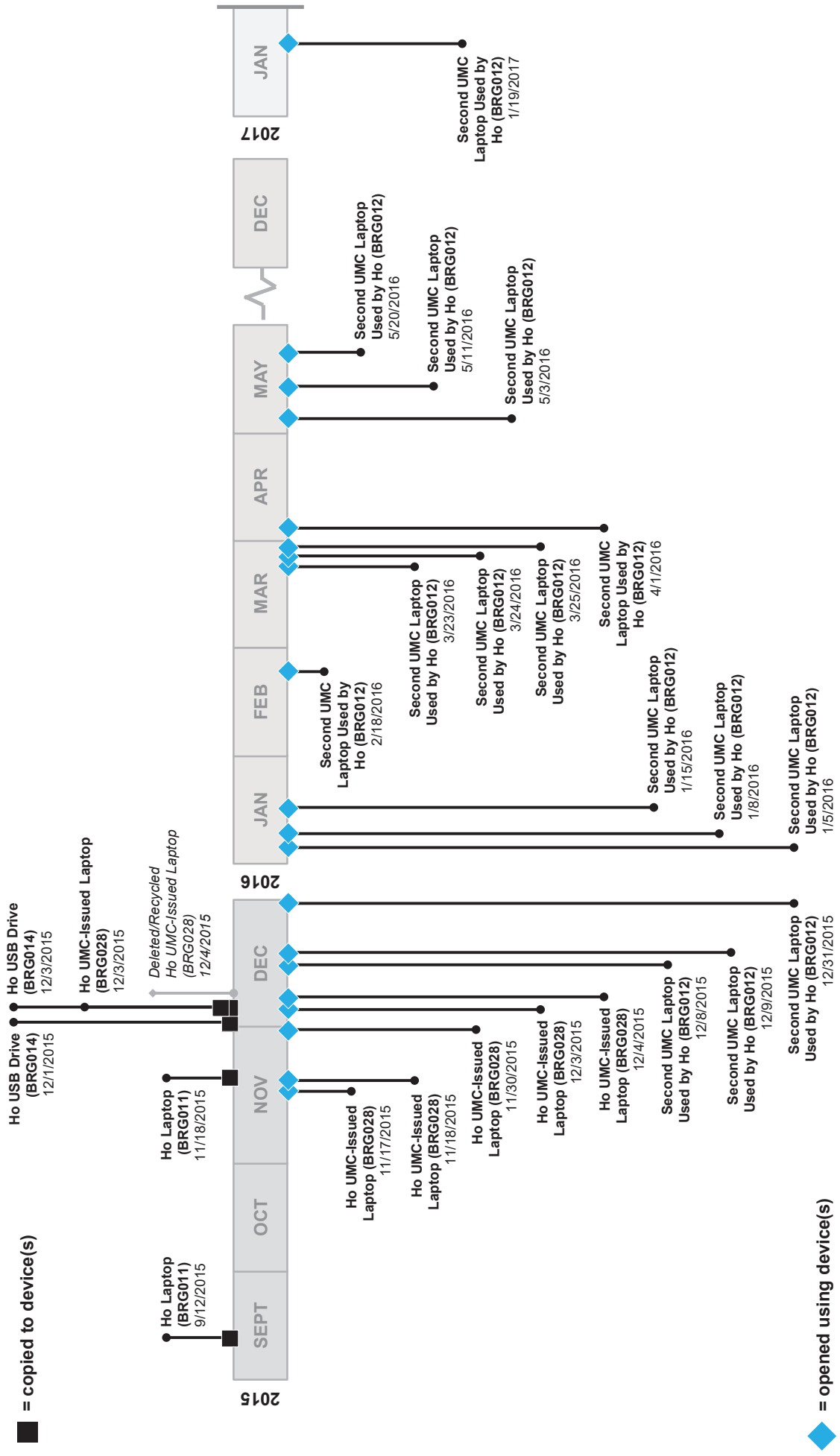

EXHIBIT B

ANDREW CRAIN REBUTTAL REPORT

I. Background

1. On July 1, 2021, I provided the Andrew Crain Expert Report (the "Crain Report"), in conjunction with the prosecution's engagement of Berkeley Research Group ("BRG") in this matter. For background, I was asked to provide in the Crain Report various opinions related to the forensic analysis that my team and I performed on digital forensic evidence provided for our review.

2. On September 10, 2021, Jinhua's disclosed expert in this matter, Mr. John Ashley, provided a disclosure statement of opinions and observations (the "Ashley Disclosure").

3. I am providing this rebuttal report in response to certain points raised in the Ashley Disclosure.

II. Summary of Rebuttal Opinions

4. The opinions I provided in the Crain Report are largely unchanged in response to the Ashley Disclosure because, at the highest level, the Ashley Disclosure did not address my findings concerning the copying and opening of numerous charged trade secret documents in this matter. Instead, the Ashley Disclosure suggested that, because some evidentiary computing devices were used after the devices were seized—and therefore certain limited evidence on those devices underwent changes— those evidentiary datasets are now unreliable. I do not agree.

5. As described more fully in the following sections, the Ashley Disclosure:

    a) Does not allege that any post-seizure access occurred whatsoever for five specific evidentiary datasets which, as described in the Crain Report, contain forensic evidence indicating copying and/or opening of all but two of the charged trade secret documents in this matter;
    b) Does not identify even a single instance in which post-seizure access rendered unreliable the forensic evidence underpinning a pre-seizure event described in the Crain Report;
    c) Identified only a single instance of a charged trade secret document being opened post-seizure.

6. Accordingly, I do not believe the post-seizure access to some of the datasets at issue, as described in the Ashley Disclosure, impacted in any way the reliability of the forensic evidence described in the Crain Report. In fact, because the post-seizure access described in the Ashley Disclosure was captured in the available metadata, and is therefore reliable in the same fashion as the data and metadata described in the Crain Report, we can be highly confident that the post-seizure access had no effect on the pre-seizure forensic evidence outlined in the Crain Report.

7. I reserve the right to amend, alter, or supplement my findings should additional evidence / information be provided to me for analysis, or to rebut testimony from defense witnesses. I also reserve the right to create demonstratives for use at trial and / or to use other graphical depictions to present my findings.

III. Post-Seizure Access to Some of the Original Data Sources Did Not Have Any Impact on the Specific Forensic Evidence Indicating the Pre-Seizure Copying and Opening Events Detailed in the Crain Report

8. The Ashley Disclosure details at length its findings related to the fact that some, but not all, of the original data sources in this matter were accessed after the date on which they were seized by Taiwanese law enforcement. But notably, as discussed more fully below, only one charged trade secret document was accessed (on a single occasion) during this post-seizure access.

9. As a general matter, I agree that proper handling of digital evidence is important, and that litigants and law enforcement personnel should strive to follow best practices with respect to the preservation and examination of digital forensic evidence. It is also a common, practical reality in the digital forensics industry, however, that original sources of digital evidence have not always been preserved in strict accordance with such best practices. As a result, certain forensic information contained in those datasets (such as date / time stamps) can be inadvertently or unwittingly changed prior to forensic imaging and examination.

10. In such instances, forensic examiners can analyze and rely on specific forensic artifacts contained within those datasets that were unaffected by such later events, and hence, remain accurate as to what occurred before. Specifically, regarding the instant matter, the post-seizure access to some of the original data sources did not affect, let alone destroy, copious and reliable forensic evidence of pertinent events on those devices that occurred *prior* to seizure. In fact, all the forensic evidence cited in the Crain Report related to pre-seizure copying and opening of the charged trade secret documents on the various devices remains unchanged by the post-seizure access described in the Ashley Disclosure. And with one minor exception unrelated to post-seizure access, the Ashley Disclosure asserts no opinion to the contrary.[1]

11. In fact, the Ashley Disclosure identified only a single instance in the Crain Report of a file opening corresponding to a charged trade secret document that occurred post-seizure (i.e. the February 13, 2017 opening of trade secret document number 5 on the BRG009 device).[2] Additional forensic evidence from the BRG009 device confirms, however, that the underlying

[1] Separate from his contentions relating to post-seizure access, the Ashley Disclosure discusses (at pp. 25-26) a specific timestamp that occurs on the BRG010 device as a possible result of a failing internal battery, causing the system clock on that device to reset to 1/1/2003 (or 12/31/2002 subject to a time-zone offset). I agree that this date stamp – 12/31/2002 – is unlikely to reflect the actual date and time of the associated event. Mr. Ashley does not assert or even suggest, however, that any of the 12/31/2002 timestamps occurred *after* seizure of BRG010. Indeed, Mr. Ashley does not assert that any post-seizure access occurred at all with respect to the BRG010 device. Furthermore, I disagree with Mr. Ashley's supposition that this occasional system clock reset due to battery failure "cause[s] all time and date metadata on the hard drive [of BRG010] to be unreliable" (Ashley Disclosure, p. 26). The Ashley Disclosure appears to then concede this point (at pp. 26-28), where it identified only 12 items from BRG010 with the date of 12/31/2002, rather than all items originating from the BRG010 source (*see, e.g.*, Crain Report Exh. D, reference nos. 59, 63, 546, 565-66 (among others) (identifying other events tied to the BRG010 device with date stamps other than 12/31/2002 and which Mr. Ashley does not identify as being "incorrect dates" [Ashley Disclosure, p. 26]).

[2] *See* Ashley Disclosure, pp. 21-22; *see also* Crain Report at ¶ 21(k).

document was not modified during this opening event.[3] That is, the evidence shows that on that date, the document was opened on BRG009 and then closed, without making or saving any changes.

12. In paragraph 4 of the Crain Report, I identified the various artifacts that my team and I used to reach the conclusions in that report. Each of those artifacts was unaffected by the post-seizure events that occurred later. This is critical because it means that the conclusions in the Crain Report are unaffected by the contentions of post-seizure access in the Ashley Disclosure. For example:

    a) File system created dates, link file created dates, and Office Alerts are not subject to modification by later events, and therefore can be relied-upon despite subsequent access to the device.

    b) Generally speaking, the file system last modification date for link files could be updated by later events (i.e., if the document in question was opened again). Yet none of findings in the Crain Report relating to the charged trade secret documents were affected by post-seizure updates to link file last modification date / time stamps.[4]

    c) The Windows jumplist artifact, akin to a ledger of files opened in the past, similarly is intact; it may show 'new' entries or show an updated embedded "last accessed" value for files opened on a device post-seizure, but none of the events relating to charged trade secret documents described in the Crain report were affected by a post-seizure entry or update in the Windows jumplist artifact.

13. Many forensic artifacts, including all the evidence relied upon in the Crain Report, provide a reliable and accurate historical record of file copying and opening. They are not overwritten or changed when other unrelated events occur on the computer. Indeed, the Ashley Disclosure itself actually confirms this -- a substantial portion of the Ashley Disclosure is dedicated to cataloging multiple events that occurred between the seizure and the forensic imaging of the evidentiary devices. The very fact that the Ashley Disclosure can conclude that some events (such as file copying, file opening, and file deletions) occurred post-seizure, irrespective of the fact that still other events occurred *even later* in time,[5] confirms that the mere existence of forensic artifacts on a computer after a particular event does not invalidate or render any less reliable the forensic evidence of previous events on that computer. Put simply, the later events *add* to the history, rather than delete or change prior history.

---

[3] The file system last modification date for this document, as stored on the BRG009 device at the folder path: /Documents and Settings/Administrator.KENNY/桌面/USB/90s/V90B/0. Design/EES Document/【DR25nmS】Design rules Periphery_EES_2012000026-013_Rev.13.xls, remains May 5, 2016. This indicates the document was not substantively modified during the opening event on February 13, 2017.

[4] The February 13, 2017 opening of Trade Secret 5 on BRG009 (*see, e.g.* Crain Report at ¶ 21(k)) was based on link file evidence that was created and modified on that date, versus created earlier and then updated on that date.

[5] *See, e.g.*, Ashley Disclosure, pp. 8-10, describing a chronology of events on BRG003 spanning multiple days post-seizure, including specific events of machine access, copying, USB insertion, and file opening.

14. In sum, the Ashley Disclosure does not identify a single instance in which post-seizure access rendered unreliable any of the forensic evidence underpinning pre-seizure findings described in the Crain Report.

IV. The Ashley Disclosure Makes No Mention of Any Post-Seizure Access to Five Datasets Identified in the Crain Report that Contain Evidence of Copying and/or Opening of Virtually All the Charged Trade Secret Documents

15. The Crain Report details forensic evidence from five datasets (BRG008,[6] BRG010,[7] BRG026,[8] BRG027,[9] and BRG028[10]) that shows copying and/or file opening events related to all but two of the charged trade secrets documents (i.e., numbers 1 (documents 4-16), 2, 3, 4, 5, 6, 7, and 8). The Ashley Disclosure makes no mention of any post-seizure access to any of these five datasets. Accordingly, as these datasets are not challenged by Mr. Ashley, I am not addressing them further.

V. The Ashley Disclosure Discusses Post-Seizure Access on Four Datasets For Which the Crain Report Asserts No Findings About Copying or Opening of Charged Trade Secrets

16. The Ashley Disclosure asserts that that data access occurred post-seizure on, among others, BRG004,[11] BRG006,[12] BRG023,[13] and BRG024.[14] The Crain Report offered no substantive opinions as to the existence or use of charged trade secrets on any of these devices. Accordingly, I am not addressing these devices further.

VI. Several Devices Discussed in the Ashley Disclosure as Being Accessed Post-Seizure Actually Show Only a Small Number of Non-Substantive, Automatic Updates, or Other Updates Not Germane to the Findings in the Crain Report

17. The Ashley Disclosure discusses that the BRG011, BRG013, and BRG014 datasets were subject to a small number of files being "created and then deleted"[15] on each device after seizure and prior to forensic imaging. This discussion leaves the reader with the impression that investigators were, for example, adding new substantive files to the devices, or were deleting substantive, user-

[6] *See, e.g.*, Crain Report, ¶¶ 16-17 and corresponding footnote(s).
[7] *See, e.g.*, Crain Report, ¶¶ 16-17 and corresponding footnote(s).
[8] *See, e.g.*, Crain Report, *passim.*
[9] *See, e.g.*, Crain Report, ¶ 15 and corresponding footnote(s).
[10] *See, e.g.*, Crain Report, *passim.*
[11] *See, e.g.*, Ashley Disclosure, pp. 11-12.
[12] *See, e.g.*, Ashley Disclosure, pp. 12-13.
[13] *See, e.g.*, Ashley Disclosure, pp. 19-20.
[14] *See, e.g.*, Ashley Disclosure, pp. 20-21.
[15] The Ashley Disclosure identifies thirty-one (31) such files for BRG011 (Ashley Disclosure at pp. 15-16 and Exh. 13), one (1) such file for BRG013 (Ashley Disclosure at pp. 17-18 and Exh. 16), and seven (7) such files for BRG014 (Ashley Disclosure at pp. 18-19 and Exh. 17).

generated files[16] ("User Documents") present on the device, thereby introducing confusion as to what data was on the device as attributable to custodial actions. However, no such confusion exists because the post-seizure actions are readily identifiable by their metadata—as is evident from the Ashley Disclosure's discussion and numerous exhibits detailing exactly those actions. In addition, the Ashley Disclosure critically fails to mention that the file creations and deletions on each of these three datasets occurred automatically, as a result of simple file opening activity and thus relate only to a small number of non-substantive files.

18. More specifically, the files that were created and deleted from the BRG011, BRG013, and BRG014 datasets after seizure are referred to as "Office owner" files, which I discussed in the Crain Report at paragraph 2.b. "Office owner" files are small temporary files which are automatically created by Microsoft Office when an Office document is opened on a computer. "Office owner" files follow the naming convention of prepending "~$" to the filename of the Word, PowerPoint, Excel, etc. file being opened, and the "Office owner" file is then automatically deleted by the computer when the underlying Office document file is closed. "Office owner" files serve to 'lock' the underlying file so that only one user can make changes at a time, to avoid data conflicts with simultaneous editing.

19. Thus, while it is true that BRG011, BRG013, and BRG014 show evidence (via these "Office owner" files) of file opening after the devices were seized, none of the "file creations or deletions" identified in the Ashley Disclosure resulted in the addition or modification of any User Documents on any of these devices. Similarly, these post-seizure "file creations and/or deletions" did not cause the deletion of any User Documents that were already on the devices when seized.

20. Finally, the Ashley Disclosure's discussion regarding other evidence of post-seizure access on BRG013 pertains only to the "last modification" date of folders—not any of the User Documents therein—or to automatic system artifacts that record file system transactions on the computer.[17] These items are also simply the automatic effects of file browsing/opening activity and did not affect the underlying substantive data on the dataset. Furthermore, these alterations would not affect—nor does the Ashley Disclosure allege that they would—any of the findings in the Crain Report with respect to these datasets.

VII. With a Single Exception, the Post-Seizure Access to Three Devices Discussed in the Ashley Disclosure Had Nothing to Do With the Charged Trade Secret Documents in This Matter

A. Post-seizure access to the datasets BRG003, BRG009, and BRG012 did not affect the reliability of the forensic evidence on those devices related to pre-seizure events, and only one post-seizure access had anything to do with the charged trade secret documents on those devices, as detailed in the Crain Report.

[16] As used here, I am referring to a category of document types that users typically create, modify, and/or review during their work on the devices, as distinct from the many operating system and application type files also contained on the devices. "User Documents" includes, for example, Microsoft Office files (such as Word, PowerPoint, Excel), as well as PDF files, emails, etc.

[17] *See* Ashley Disclosure, Exh. 16.

21. The Ashley Disclosure details various post-seizure access to three datasets—BRG003, BRG009, and BRG012—including files and folders being created and deleted on those devices.[18] As described earlier, however, none of this post-seizure activity had any effect on the reliability or accuracy of the forensic evidence, as described in the Crain Report, showing that each of these devices had been used prior to seizure to copy and/or access to charged trade secret documents.[19]

22. Moreover, for all of the post-seizure access described in the Ashley Disclosure, Mr. Ashley points to only a single instance of a single charged trade secret document which was impacted in any way -- when charged trade secret number 5 was opened on February 13, 2017 on the BRG009 device.[20] Furthermore, that single event was solely an opening event—the substantive content of charged trade secret number 5 on BRG009 was not changed in any way on February 13, 2017.[21]

23. Stated differently, of the more than 180 specific events detailed in the Crain Report[22] involving copying or opening of charged trade secret documents, the Ashley Disclosure points out that only one of those events took place after the subject devices were seized, and the forensic evidence establishes that that event did not change the actual content of the file involved.

24. In addition, closer analysis of the other files and folders whose date/time stamps were updated during post-seizure access reveals a somewhat different story than what the Ashley Disclosure leads the reader to believe. For one device, BRG003, more than 93% of the files which were created during post-seizure access were the result of Taiwanese MJIB saving a copy of a network share at UMC to the device.[23] For the other two devices, BRG009 and BRG012, all of the files and folders that were created post-seizure consist solely of system-type files (not User Documents), and created automatically via booting and operation of the computer.[24] And for all three devices, all of the files and folders that the Ashley Disclosure asserts were deleted during post-seizure access consist entirely of temporary and system files, rather than User Documents.[25]

---

[18] *See, e.g.*, Ashley Disclosure, pp. 8-11 and Exh. 6 (relating to BRG003), pp.13-15 and Exh. 11 (relating to BRG009), pp. 16-17 and Exh. 14 (relating to BRG012).
[19] *See, e.g.*, Crain Report, pp. 11-12 (detailing evidence on the BRG003 device regarding charged trade secret documents 5, 6, and 7), pp. 7-13 (detailing evidence on the BRG009 device regarding charged trade secret documents 1 (numbers 2, 3, 6, 8-16), and 2-8), and pp. 8-13 (detailing evidence on the BRG012 device regarding charged trade secret documents 1 (numbers 4-7, 10-16) and 5-8).
[20] Discussed above in ¶ 11.
[21] The file system last modification date for this document, as stored on the BRG009 device at the folder path: /Documents and Settings/Administrator.KENNY/桌面/USB/90s/V90B/0. Design/EES Document/【DR25nmS】Design rules Periphery_EES_2012000026-013_Rev.13.xls, remains May 5, 2016. This indicates the document was not substantively modified during the opening event on February 13, 2017.
[22] *See* Crain Report, ¶¶ 11-25.
[23] *See* Ashley Disclosure, pp. 8-11 and Exh. 6.
[24] *See* Ashley Disclosure, Exhs. 11, 14.
[25] *See* Ashley Disclosure, Exhs. 6, 11, 14.

25. The below chart summarizes the more detailed context of the post-seizure access on the BRG003, BRG009, and BRG012 datasets:

Events During Post-Seizure Access	BRG003[26]	BRG009[27]	BRG012[28]
Files/Folders Created Post-Seizure	34,905	91	160
Files/Folders Created Due to UMC Network-Share Download Post-Seizure	32,688 (> 93%)	0	0
System/Temporary Files/Folders Created Post-Seizure[29]	2,100+	91	160
Files/Folders Deleted Post-Seizure	1,267	15	21
System/Temporary Files/Folders Deleted Post-Seizure	1,267	15	21
Charged Trade Secret Files Created Post-Seizure	0	0	0
Charged Trade Secret Files Modified Post-Seizure	0	0	0
Charged Trade Secret Files Deleted Post-Seizure	0	0	0

B. The Ashley Disclosure alludes to potential spoliation of evidence owing to post-seizure access, yet fails to identify any forensic evidence that was lost, or was likely to have been lost, and which may have been helpful to Defendants

26. The Ashley Disclosure repeatedly asserts that post-seizure access amounts to a loss of relevant evidence on various devices.[30] With respect to one device – BRG003 – the Ashley Disclosure points out that significant data volume was added post-seizure, and that this newly added data may have overwritten previously-existing data within that storage space.[31] While this is correct from a technical standpoint, the Ashley Disclosure cites no forensic evidence indicating that any data was actually lost, nor does the Ashley Disclosure attempt to identify what type of data may have been lost that would have been pertinent to his forensic examination or would otherwise bear on the findings in the Crain Report. Again, it also did not impact any of the charged trade secret documents, as depicted in the chart above.

//

//

[26] *See* Ashley Disclosure, p. 8 and Exh. 6.
[27] *See* Ashley Disclosure, p. 13 and Exh. 11.
[28] *See* Ashley Disclosure, p. 16 and Exh. 14.
[29] The BRG003 device contains approximately 15-20 User Documents that were created post-seizure in the "Desktop" folder of Mr. Wang's user profile (46685), and which were not part of the download of the "NBD" UMC network share. *See also* Ashley Disclosure, Exh. 6.
[30] *See* Ashley Disclosure, pp. 7-8, 11, 20, 21. As discussed earlier, however, the post-seizure effects for numerous of the evidentiary devices pertained to either a small number of non-substantive "Office Owner" files, or to devices about which the Crain Report asserted no findings.
[31] *See, e.g.*, Ashley Disclosure, pp. 7-8, 11, 31-32.

VIII. Excluding Post-Seizure Opening Events From the 'Company' Embedded Metadata Analysis Described in the Crain Report Still Shows Hundreds of File Openings Before The Devices Were Seized

27. The Crain Report detailed certain forensic evidence showing that files responsive to specific criteria (such as a particular value in the "company" embedded metadata field or containing the phrase "Micron confidential") were opened on various devices.[32] The Ashley Disclosure discussed that some of these file opening events occurred either post-seizure, or in the case of the BRG010 device, were associated with date / time stamps from 2002.[33]

28. Even excluding the post-seizure and 2002 events discussed in the Ashley Disclosure, the forensic evidence in this matter clearly shows that hundreds of document instances were opened that meet either/both these criteria. With these exclusions, the numbers in the Crain Report can be revised as follows:

    a) Crain Report, paragraph 7: This analysis determined that at least 439 document instances in the evidentiary population were: (a) opened one or more times; and (b) contained a responsive value in the "company" embedded metadata field.

    b) Crain Report, paragraph 8: Similarly, this analysis determined that at least 255 document instances in the evidentiary population were: (a) opened one or more times; and (b) contained the phrase "Micron confidential."

    The findings in paragraph 9 of the Crain Report, about the document instances opened using Mr. Ho's user profile, are unaffected by any post-seizure access to the devices (or the issue of 2002 date on the BRG010 device).

29. Other than file opening events that occurred post-seizure or were associated with 2002 (with regard to BRG010), the Ashley Disclosure did not address these hundreds of instances where documents were opened that met these criteria, as was detailed in the Crain Report.

IX. The Crain Report Did Not Address Certain USB Devices That Were Connected to Computers Post-Seizure Because No Evidence Was Found Suggesting Those Devices Contained Charged Trade Secret Documents

30. The Crain Report included findings related to three "unrecovered" USB devices, including the forensic evidence indicating these devices contained one or more of the charged trade secret documents.[34] The Ashley Disclosure (at pages 29-30) detailed 10 USB devices that were connected to various computers in this matter on dates/times post-dating the seizure of those computers. And of these 10 USB devices, eight were not provided for analysis by my team or Mr.

[32] *See* Crain Report, ¶¶ 6-9 and Exh. D.
[33] *See* Ashley Disclosure, pp. 22-28.
[34] *See* Crain Report, ¶ 10.

Ashley's team.[35] The Ashley Disclosure then critiques the Crain Report for failing to mention these USB devices that were connected post-seizure. Simply put, the Crain Report did not address these eight USB devices (i.e. that were connected post-seizure, but which were not provided for analysis) because my team and I did not find any evidence indicating that they contained any of the charged trade secret documents (and hence, would not have been a potential source for any of the charged trade secret documents to be copied *on* to the computers).

X. The Ashley Disclosure Includes Additional Incomplete and/or Inaccurate Statements

31. The Ashley Disclosure asserts that the custodian of the BRG014 device was "erroneously list[ed]" in the Crain Report as Ho Jianting (JT Ho), where one documentary source indicates that the device is owned by Kenny Wang.[36] However, while the Ashley Disclosure correctly cites one document, it fails to mention that this information stands in direct conflict with another document, the FBI's Verbatim Translation of the Bill of Indictment of Taichung District Prosecutors Office, Taiwan, which describes the BRG014 device as being "owned by HO Jianting"[37] (capitalization in original).

32. Furthermore, this uncertainty in determining the custodial association of devices is why forensic examiners often analyze the underlying data stored on the device, to 'associate' the device to one custodian or another, even if it cannot confirm legal 'ownership.' The Crain Report included as Exhibit C the analysis performed by my team to attempt to confirm the association of BRG014, which shows multiple independent indicia of the device having been used by JT Ho (including presence of Ho's email on the drive and repeated use of the drive on a computer assigned to Ho and on which Ho – but not Wang – had a user profile). The Ashley Disclosure offers no opinion as to the analysis and findings described in Exhibit C to the Crain Report.

33. The Ashley Disclosure also repeatedly misrepresents the character of files which were "created and then deleted" from various devices. The net effect of the Ashley Disclosure is that the reader is left with the impression that substantive data related to the files in the custodians' possession was added and/or deleted after these devices were seized. Notably, the Ashley Disclosure appears to disregard the critical distinction between a *substantive Microsoft Office file* and the *non-substantive "Office owner" file* (discussed above) that is automatically created and deleted while opening an Office document. In particular:

---

[35] *See* Ashley Disclosure, pp. 29-30.

[36] *See* Ashley Disclosure, p. 19 ("Mr. Crain in his report in *Table 1: List of Frequently Referenced Evidence Items* erroneously lists the Custodian of BRG014 to be Ho Jianting (JT Ho), when the table in Exhibit 2, Page 51 to the Micron Complaint clearly lists the owner of the device as Kenny Wang."); *see also* Ex. 2, Page 51 to the Micron Complaint (the Indictment Decision of Taiwan Taichung District Prosecutors Office, describing a "USB (Kingston brand)" which is "[o]wned by Kenny Wang" and whose "electronic records" were stored "under USB \106030-25-14\").

[37] *See* FBI's Verbatim Translation of the Bill of Indictment of Taichung District Prosecutors Office, Taiwan, at p. 35, describing a "Mobile disk (Kingston brand)" that "is owned by HO Jianting" and whose "electromagnetic records are stored in \106030-25-14\").

a) Page 12 of the Ashley Disclosure describes the review of materials on BRG006 on 2/13/2017 which resulted in the "creat[ion] and then delet[ion of] the file titled Fab11_twr_materials_for_25nm_task_force_V6.pptx." However, the file called 'Fab11_twr_materials_for_25nm_task_force_V6.pptx' was neither created on 2/13/2017 on BRG006, nor was it deleted at any point – it is still active on the device.[38] The file created and deleted on the device on 2/13/2017 was only the small non-substantive "Office owner" file called "~$Fab11_twr_materials_for_25nm_task_force_V6.pptx."[39]

b) Page 18 of the Ashley Disclosure makes the same allegation that a specific file on BRG013 being reviewed by the MJIB "is the file that was created and then deleted" during examination.[40] However, the substantive file Mr. Ashley described was not created or modified on the device post-seizure, nor was it deleted at any point; only the small non-substantive "Office owner" file was created and deleted.[41]

c) Page 19 of the Ashley Disclosure makes the same allegation as to two specific files on BRG014 being reviewed by the MJIB as "two of the files where were created and then deleted from the device."[42] However, the two substantive files Mr. Ashley discussed were not created or modified on the device post-seizure, nor were they deleted at any point; only the small non-substantive "Office owner" files were created and deleted.[43]

Dated: October 15, 2021

Andrew Crain

[38] *See* Ashley Disclosure, Exh. 10 (showing file was created 1/15/14 19:00 and not deleted).
[39] *Id.*
[40] *See* Ashley Disclosure, p. 18 ("It is apparent from the transcript of the MJIB interrogation of the Micron employee Yi-Leng Chen that he actually reviewed the files and folders on this device which had their metadata altered. In his answer at the bottom of page 4 of the interrogation transcript he **specifically references the file \4GLP2\WT\4GMLP2A_Category_Bin_define_Ver0A (Non-C-comp)_vl.xlsm, which is the file that was created and then deleted from the device**.") (emphasis added).
[41] *See* Ashley Disclosure, Exh. 16 (which does *not* list the file "4GMLP2A_Category_Bin_define_Ver0A (Non-C-comp)_vl.xlsm," because that file was not created or modified after seizure, but does list the corresponding "Office owner" file "~$4GMLP2A_Category_Bin_define_Ver0A(Non-C-comp)_v1.xlsm").
[42] *See* Ashley Disclosure, p. 19 ("It is apparent from the transcript of the MJIB interrogation of Micron employee Yi-Leng Chen that he actually reviewed the files and folders on this device which were created and then deleted from the device. In his answer at the bottom of page 4 and the top of page 5 of the interrogation transcript he **specifically references the files DRAM data\DRAM flow data\cell dummy\ECD-2013000667-001_25nmS_6F2_MemoryCel.ppt (*sic*) and80series_dram_overview_and_comparison.pptx (*sic*) which are two of the files which were created and then deleted from the device**.") (emphasis added; errors in original).
[43] *See* Ashley Disclosure, Exh. 17 (which does *not* list either file, because neither file was created or modified after seizure, but does list the corresponding "Office owner" files "~$ECD-2013000667-001_25nmS_6F2_MemoryCell.ppt" and ~$80series_dram_overview_and_comparison.pptx")